SUMMARY OF SECTION 7

CONFIDENTIALITY AND INFORMATION GOVERNANCE

7	Confidentiality and Information Governance
7.01	IT Security Policy
7.02	Corporate Records Policy
7.03	REMOVED MAY 2011
7.04	Safe & Secure Handling of Confidential Information
7.05	Information Lifecycle Policy
7.06	Clinical Records Management Policy & Procedure
7.07	Operation of a Registration Authority Policy
7.08	Information Services Data Quality Policy
7.09	REMOVED MAY 2011
7.10	Information Technology Acceptable Use Policy and Procedure
7.11	Mobile and Remote Access Working Security Policy and Procedure
7.12	Digital Investigations Policy and Procedure
7.13	Freedom of Information Act Policy
7.14	Email / Internet General Policy
7.15	Information Governance Policy
7.16	Information Risk Policy

Information Sharing with Other Agencies Policy (Incorporating Individual Agreement Protocols) (can be found under **PROTOCOLS & PROCEDURES WITH EXTERNAL AGENCIES)**
Generic Information Sharing Protocol with Nottinghamshire Police (can be found under **PROTOCOLS & PROCEDURES WITH EXTERNAL AGENCIES**)
Generic Information Sharing Protocol with Nottinghamshire Police - Process Documentation (can be found under **PROTOCOLS & PROCEDURES WITH EXTERNAL AGENCIES**)

The Champion for this section is the Executive Director Nursing and Allied Health Professionals

Review Date: 2012

INTRODUCTION

There are a range of complex legal and professional obligations that limit, or set conditions in respect of the management, security, use and disclosure of information along with a range of statues that permit or require information to be used or disclosed. Information Governance is a framework that integrates these separate but interrelated acts, directives and regulations within a single transparent package. This framework currently encompasses; Records Management, Information Requests (clinical and non clinical), Security, Data Quality and Information Sharing although this list is not exhaustive. Each area has different legal and professional obligations which individuals need to consider on an individual basis. The role of the Trusts Caldicott Guardian (Peter Miller) and the Trusts Senior Information Risk Owner (Peter Miller) along with the Trusts Information Governance and IT Security Departments is to support colleagues in considering the varying aspects of governance, balancing the practicality and care of our patients whilst keeping the Trusts information assets safe and secure.

Safeguarding of Trust assets such as information, equipment, and Data networks is paramount in ensuring that we can provide sufficient assurance that information provided by Patients, their families, staff and sensitive corporate documentation will only be used for the purposes for which it was originally given, and not released to others without their consent.

7.01 INFORMATION SECURITY SYSTEMS POLICY

This policy aims to detail how the Trust meets its legal obligations and NHS requirements for information security standards. The requirements within the policy are primarily driven by the Data Protection Act 1998 that is the key piece of legislation covering security and confidentiality of personal information.

7.02 CORPORATE RECORDS POLICY

NHS Organisations have a statutory duty to ensure arrangements for the safekeeping and eventual disposal of their records in both electronic and manual formats. The purpose of this policy is to provide information, highlight the principles involved and advise colleagues on version control, creation, using, filing systems, retention and eventually disposing of its Corporate Records. The Policy also sets out the **minimum** periods for which various records created within the Trust or by its predecessor bodies should be retained.

7.03 COPYING LETTERS TO PATIENTS

REMOVED MAY 2011

7.04 SAFE AND SECURE HANDLING OF CONFIDENTIAL INFORMATION POLICY

The policy aims to cover the safe and secure handling of confidential information (clinical and non clinical) which is used in support of the Trust's Business needs. A Safe Haven Policy ensures the privacy and confidentiality of information and to adhere to legal restrictions placed upon the Trust. All staff in the Trust must safeguard the integrity, confidentiality and availability, of personal and or sensitive information. This policy does not replace any existing policies or procedures safeguarding information for clinical and non-clinical purposes but enhances existing practice.

7.05 INFORMATION LIFECYCLE

This document sets out a framework within which all staff responsible for managing the Trust's information can develop specific policies and procedures to ensure that information is managed and controlled effectively, and at best value, commensurate with legal, operational and information lifecycle management needs.

This policy relates to all clinical and non-clinical operational records held in any format by the Trust. It explains the responsibilities of managers and staff.

7.06 CLINICAL RECORDS MANAGEMENT

The purpose of this policy is to provide information and to support colleagues on records management in line with legal obligations, NHS requirements and circulars. The management of the Trust's clinical records supports the delivery of high quality care retrieval and security of this information is clearly highlighted. The policy provides guidance on the pathway for records management from creation to destruction either in paper or electronic format clarifying which documentation and records should not be included along with accountability of all staff both professionally and personally.

7.07 OPERATION OF A REGISTRATION AUTHORITY
This policy sets out the requirements for staff to register with the Registration Authority outlining the background, legislation and process needs ensuring that all aspects of registration services and operations are performed in accordance with National Policies and procedures. Provision for controls over the issue and maintenance of electronic Smartcards, whilst providing and efficient and responsive service that meets the needs of the users.

7.08 DATA QUALITY POLICY
This policy describes the measures that all Trust information systems owners must implement to achieve appropriate levels of quality in support of the Trusts business needs. In particular, systems that impact on clinical, financial or safety issues must adhere to the highest possible levels of quality at all times.

7.09 CLINICAL CODING DATA QUALITY POLICY
REMOVED MAY 2011

7.10 INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY & PROCEDURE
This policy and procedure has been developed to meet legal requirements and good practice around the use of Information Technology Equipment. It is also designed to satisfy NHS obligations by adhering to Caldicott principles. It has been developed to promote good practice and to reduce the potential liabilities arising from misuse.

7.11 MOBILE AND REMOTE ACCESS WORKING SECURITY POLICY & PROCEDURE
This policy has been designed to detail the data security requirements that must be adhered to by staff when working from remote locations or using mobile computer equipment.

7.12 DIGITAL INVESTIGATIONS POLICY AND PROCEDURE
The almost ubiquitous use of ICT systems within the Trust has meant that digital evidence is very likely to feature in a wide range of investigations within the Trust. When gathering digital evidence it is vital that it is collected in a fair, legal and admissible.

7.13 FREEDOM OF INFORMATION ACT POLICY
The aim of this policy is to ensure staff are aware of their responsibilities under the Freedom of Information Act 2000. To establish the Trusts publication scheme which highlights information that is publicly available providing a transparent view of records which fall into the public domain reducing external access requests.

7.14 EMAIL / INTERNET GENERAL POLICY
This policy and procedure has been developed to meet legal requirements and good practice around electronic communications (email and Internet) and to reduce the potential liabilities arising from misuse. Provide clear guidance for employees about their responsibilities, when using electronic communications, this policy sets out the principles to be followed at all times

7.15 INFORMATION GOVERNANCE POLICY
This Policy aims to detail how the Trust meets its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the Data Protection Act 1998 that is the key piece of legislation covering security and confidentiality of personal information

7.16 INFORMATION RISK POLICY
Information risk management is an essential element of broader information governance and is an integral part of good management practice. The intent is to embed information risk management in a very practical way into business processes and functions. This is achieved through key approval and review processes / controls – and not to impose risk management as an extra requirement.